

## CITY OF SAN ANTONIO



### Administrative Directive

### AD 7.8B Information Security Program

### Procedural Guidelines

Guidelines to establish responsibility for the protection of information resources.

### Department/Division

Information Technology Services Department (ITSD)

### Effective Date

July 6, 2009

### Project Manager

John Byers, Chief Information Security Officer (CISO)

## Purpose

The purpose of this directive is to establish responsibility and provide general guidance for all of Information Technology Services Department (ITSD) and City of San Antonio (COSA) employees for the protection of information resources entrusted to each person in the performance of City business. This directive summary works together with all other information security directives.

## Policy

This directive provides the requirements and guidelines to assist in accomplishing the goals of the IT security program (ITSP). Information security works together with the physical security to establish standards, procedures, and directives that provide the foundation for COSA security.

## Policy Applies To

☐ External & Internal Applicants

☒ Current Temporary Employees

☒ Current Full-Time Employees

☐ Current Volunteers

☒ Current Part-Time Employees

☒ Current Grant-Funded Employees

☒ Current Paid and Unpaid Interns

☒ Police and Fire Academy Trainees

☒ Uniformed Employees Under Collective Bargaining Agreements

## Definitions

N/A

## Policy Guidelines

### **General Guidelines:**

#### A. Enterprise Breadth

1. The ITSP shall set the foundation for a COSA implementation of administrative, physical, and technical safeguards to reduce IT security risks and vulnerabilities to a reasonable and appropriate level based on the sensitivity and criticality of data stored on, processed by, or transmitted through the City IT resources.

#### B. Documented Controls

1. Information security directives, procedures, and guidelines shall be written in support of the program and generate a minimum set of safeguards (security controls) common to the entire City.
2. The ITSP shall require the deployment of technical and non-technical controls, as well as the processes the program uses for daily operations and maintenance to be documented.

#### C. Incorporate Risk Management Principles

1. The program shall incorporate the principles of risk management so that when the controls are applied, information owners and/or IT resource owners acknowledge that the controls provide an “acceptable level of risk” against known threats to the confidentiality, integrity, and availability of the information and/or information resources.

#### D. Tactical and Strategic Planning

1. The ITSP shall require tactical (short term – six months) and strategic (long term – three years) information security planning.

#### E. ITSP Plans

1. Shall address tactical and strategic information security requirements to protect networks, facilities, systems, or groups of information systems that belong to the City.
2. Shall align with the overall IT strategic plan of the City. The plans shall be updated to reflect changes in the environment and security requirements.

#### F. Awareness and Training

1. The ITSP shall include topics for information security awareness and training. The program shall require training and awareness materials that address COSA information security requirements. To the extent possible, the program shall assist with requests for unique training materials.

#### G. Control Objectives and Metrics

1. The ITSP shall establish COSA-wide IT control objectives and

metrics that can be used to measure the effectiveness of the program or deployed controls.

#### H. Incident Reporting and Response

1. The ITSP shall require the creation, implementation, testing, and maintenance of an incident response capability for COSA. The capability shall be adaptable to all departments of COSA.
2. The incident response capability should be able to prevent, detect, contain, and correct security-related events and incidents that threaten the confidentiality, availability, or integrity of information.

#### I. Program Monitoring and Adjustment

1. The ITSP shall be regularly monitored by internal processes and by independent reviews.
2. The program shall require a documented process for planning, implementing, evaluating, and recording remedial actions to address deficiencies.
3. Reviews using independent security specialists may be employed periodically to provide an unbiased review of the presence and effectiveness of the program's controls. Results of monitoring shall be assessed to identify:
  - a. Immediate corrective actions that may require coordination and approval
  - b. Required adjustments to specific security controls
  - c. Required adjustments to tactical or strategic plans

#### J. Communications

1. The ITSP shall prescribe a process to communicate information security matters both internally and externally.
2. Reports on the program's activities, progress, and shortfalls shall be presented annually to the Chief Information Officer (CIO).

#### K. Communication and Training Statement

1. All IT resource users shall receive training regarding the IT security program prior to gaining access to IT resources. This directive shall be made available online at [http://www.sanantonio.gov/hr/admin\\_directives](http://www.sanantonio.gov/hr/admin_directives) to all IT resource users, with cross references to the COSA ITSD departmental website.

#### L. Guidance for requesting exceptions to or deviations from this directive is outlined in *AD 7.5A Establishing IT-Related Directives*



## Roles & Responsibilities

### Chief Information Security Officer

- A. Review this directive annually, at a minimum, for both consistency and accuracy
- B. Interpret and apply this directive under the direction of the Chief Information Officer (CIO) and/or the Chief Technology Officer (CTO), as appropriate
- C. Modify or amend this directive at any time pending formal review and approval as defined in *AD 7.5A Establishing IT-Related Directives*
- D. Provide adequate notice of any such modifications or amendments
- E. Ensure the current version of this directive is posted in a public location accessible to all authorized City personnel
- F. Oversee and monitor all training, in general
- G. Report annually on the program's activities, progress, and shortfalls to the Chief Information Officer (CIO) and Chief Technology Officer (CTO)

### Departments

- A. Responsible for any disciplinary action taken against employees who violate this directive

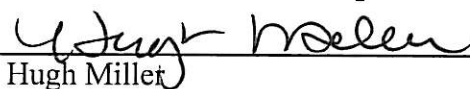
### Human Resources

- A. Provide guidance, as required, to City departments regarding appropriate disciplinary action to be taken against employees who violate this directive

## Attachments

N/A

Information and/or clarification may be obtained by contacting the Information Technology Services Department (ITSD) at 207-8301.

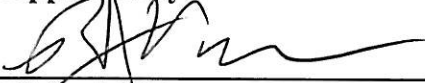


Hugh Miller  
Information Technology Services Department Director / CTO

09/14/2009

Date

Approved by:



Richard J. Varn  
Chief Information Officer (CIO)

09/16/2009

Date

Approved by:

Sheryl Sculley  
City Manager



9-29-09

Date